(54) Title: DIGITAL ACTIVE ADVERTISING

(57) Abstract

A complete system (200) for the purchasing of goods or information over a computer network (67) is presented. Merchant computers (63, 64) on the network (67) maintain databases of digital advertisements (65, 66) that are accessed by buyer computers (61, 62). In response to user inquiries, buyer computers (61, 62) retrieve and display advertisements from merchant computers (63, 64). A digital advertisement can include a program that is interpreted by a buyer's computer (61, 62). The buyer computers (61, 62) allow the users to purchase the product described by an advertisement. The form of payment can be requested after a purchase is initiated. A payment system (300) performs payment authorization. The payment system obtains account authorizations from an external financial system. Payment orders are signed with authenticators.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic	SD	Sudan
CG	Congo		of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

- 1 -

DIGITAL ACTIVE ADVERTISING
BACKGROUND OF THE INVENTION

5   The recent rapid growth of information
applications on international public packet-switched
computer networks such as the Internet suggests that
public computer networks have the potential to establish
a new kind of open marketplace for goods and services.
10   Such a marketplace could be created with a network sales
system that comprises a plurality of buyer and merchant
computers, means for the users of the buyer computers to
display digital advertisements from the merchant
computers, and means for the users to purchase products
15   described by the advertisements.

A network based sales system will need to allow
users to preview products at little or no cost, and will
need to make a large number of product advertisements
available in a convenient manner. In addition, the
20   shopping system will need to include easy-to-use
facilities for a user to purchase desired products using
a merchant independent payment method. In addition the
network sales will need to allow new buyers and merchants
to enter the market.

25   A central requirement for a marketplace is a
payment mechanism, but at present no merchant independent
payment mechanism is available for computer networks that
permits users to utilize conventional financial
instruments such as credit cards, debit cards, and demand
30   deposit account balances. We expect that both retail
payment and wholesale payment mechanisms will be required
for networks, with consumers using the retail mechanism
for modest size purchases, and institutions using the
wholesale mechanism for performing settlement between
35   trading partners. For wide acceptance the retail
mechanism will need to be a logical evolution of existing

- 2 -

credit-card, debit-card, and Automated Clearing House
facilities, while for acceptance the wholesale mechanism
will need to be an evolved version of corporate
electronic funds transfer.

5   These problems of have been approached in the
past by network based sales systems wherein, for example,
each merchant maintains an account for each user. A user
must establish an account with each merchant in advance
in order to be able to utilize the merchant. The prior

10 art network based sales systems are not designed to allow
users to use their existing credit card and demand
deposit accounts for payment, nor are they designed to
allow for programs to be included in digital
advertisements.

15   According, therefore, it is a primary objective
of this invention to provide a user interactive network
sales system in which the user can freely use any
merchant of choice and utilize existing financial
instruments for payment. Other objects include a network

20 sales system which provides a high-quality user
interface, which provides users with a wide variety and
large volume of advertisements, which is easily
extensible to new services, and which is easily expanded
to new applications within the existing infrastructure of

25 the system.

            Still other objects of the invention are to
provide a network payment system that will authorize
payment orders and remove part of the risk of fraud from
merchants.

30   An unavoidable property of public computer
networks is that they are comprised of switching,
transmission, and host computer components controlled by
many individuals and organizations. Thus it is
impossible for a network payment system to depend upon a

35 specified minimum required degree of software, hardware,

- 3 -

and physical security for all of the components in a
public network. For example, secret keys stored in a
given user's personal computer can be compromised,
switches can be tampered with to redirect traffic, and
5 transmission facilities can be intercepted and
manipulated.

The risk of performing retail payment in a public
network is compounded by statutes that make a payment
system operator in part liable for the security lapses of
10 its users. Existing Federal statutes in the United
States, including the Electronic Funds Transfer Act and
the Consumer Credit Protection Act, require the operator
of a payment mechanism to limit consumer liability in
many cases. Payment system operators may have other
15 fiduciary responsibilities for wholesale transactions.
Similar responsibilities exist in other countries for
retail and wholesale transactions.

In existing credit card payment systems, a credit
card's issuing bank takes on the fraud risk associated
20 with misuse of the card when a merchant follows
established card acceptance protocols. Acceptance
protocols can include verifying a card holder's signature
on the back of their card and obtaining authorization for
payments over a certain value. However, in network based
25 commerce a merchant can not physically examine a
purchasers credit card, and thus the fraud risk may
revert to the merchant in so called "card not present"
transactions. Many merchants can not qualify to take
this risk because of their limited financial resources.
30 Thus the invention is important to allow many merchants
to participate in network based commerce.

Other objects of the invention include utilizing
existing financial instruments such as credit cards,
debit cards, and demand deposit accounts for merchant
35 payments.

- 4 -

Existing network payment systems do not connect
to the financial system for authorization and are not
compatible with conventional financial instruments.
Existing network payment systems include the Simple
5 Network Payment Protocol [Dukach, S., SNPP: A Simple
Network Payment Protocol, MIT Laboratory for Computer
Science, Cambridge, MA, 1993.], Sirbu's Internet Billing
Server [Sirbu, M. A., Internet Billing Service Design and
Prototype Implementation, Information Networking Program,
10 Carnegie-Mellon University, 1993], and NetCash [Medvinsy,
G., and Newman, B. C., NetCash: A Design for Practical
Electronic Currency on the Internet, Proc. 1st ACM Conf.
on Comp. and Comm. Security, November, 1993].

A further object of the invention is to allow
15 users in an untrusted network environment to use
conventional financial instruments without requiring
modification to existing financial system networks.

The following definitions apply to the present
invention. A principal is a person, company,
20 institution, or other entity that is authorized to
transact business as part of a network payment system. A
payment order describes the identity of a sender, a
payment amount, a beneficiary, and a sender unique once.
A sender is a principal making a payment. A beneficiary
25 is a principal to be paid by the payment system. A
sender unique nonce is an identifier that is used only
once by a given sender. An example of sender unique
nonces are unique timestamps. An external account is an
account that can be used to settle a payment order for
30 either a sender or a beneficiary in the external
financial system. Examples of external accounts include
demand deposit accounts and credit card accounts. An
external device is a physical object that is kept in the
possession of a user for the purpose of identifying the
35 user.

- 5 -

A network payment system is a service that
authorizes and executes digital payment orders that are
backed by external accounts. A payment system
authenticates a payment order, checks for sufficient
5   funds or credit, and then originates funds transfer
transactions to carry out the payment order. A payment
system acknowledges acceptance or rejection of a payment
order. More than one payment system may exist on a
given network, and a given payment system may operate on
10   more than one host to increase its reliability,
availability, and performance. An authenticator is a
digital value that is appended to a payment order and
becomes part of the payment order that authenticates the
payment order as genuine.

15   SUMMARY OF THE INVENTION

The invention relates to a network sales system
for enabling users to purchase products using a plurality
of buyer computers that communicate over a network with a
plurality of merchant computers. Each merchant computer
20   has a database of digital advertisements. Each digital
advertisement includes a price and a product abstract.
Buyer computers request, display, and respond to digital
advertisements from merchant computers. Users can
purchase products with their buyer computers after they
25   have specified an account to pay for the purchase. A
network payment service is used to authorize the purchase
before merchant fulfillment is performed.

In a particular aspect of the invention, the
merchant computer can request account information when it
30   is not provided by the buyer computer. In another
aspect of the invention, the buyer computer can present
to a merchant a pre-authorized payment order that is
obtained from a network payment system.

In another aspect of the invention, an electronic
35   sales system contains digital advertisements that include

- 6 -

programs. The programs are executed on behalf of a user by a buyer computer, and can lead to a purchase request directed to a merchant computer that performs product fulfillment.

5   In another aspect of the invention a network payment system executes payment orders. A payment order includes a sender, a beneficiary, a payment amount, and a nonce identifier. A payment order is signed by a client computer with an authenticator that is checked by the
10   payment system. Payment orders are backed by accounts in the banking system, and are authorized by the network payment system by sending messages into a financial authorization network that knows the status of these accounts. The payment system accomplishes settlement by
15   sending messages into an existing financial system network.

In another aspect, payment orders are authenticated based on the delivery address they specify. In another aspect, the payment system will specify in its
20   authorization legal delivery addresses. In another aspect, authenticators for payment orders are based on one-time transaction identifiers that are known only to the user and the payment system. In another aspect, payment orders for a given sender are only accepted from
25   certain client computer network addresses. In another aspect, the network payment system sends messages into a financial authorization system in real-time before the network payment system will authorize a payment order.

BRIEF DESCRIPTION OF THE DRAWINGS

30   Other objects, features, and advantages of the invention will appear from the following description taken together with the drawings in which:

Figure 1 is a block diagram of a typical network sales system in accordance with the invention;

- 7 -

Figure 2 is a screen snapshot of a buyer computer display of an overview page from a merchant computer;

Figure 3 is a screen snapshot of a buyer computer display of a page of digital advertisements from a
5 merchant computer;

Figure 4 is a screen snapshot of a buyer computer display of an account query page;

Figure 5 is a screen snapshot of a buyer computer display of a fulfillment page;

10 Figure 6 is a flow chart illustrating the processing of a sale between a buyer computer and a merchant computer;

Figure 7 is a flow chart illustrating the alternate processing of payment order means for obtaining
15 missing payment information;

Figure 8 is a screen snapshot of a buyer computer display of an overview page from a merchant computer that contains a query input by the user;

Figure 9 is a screen snapshot of a buyer computer
20 display of digital advertisements in response to a user's query;

Figure 10 is a screen snapshot of a buyer computer screen of a purchase confirmation;

Figure 11 is a screen snapshot of a buyer display
25 of a fulfillment page like Figure 5;

Figure 12 is a flow chart illustrating an alternate processing of a sale between a buyer computer and a merchant computer where a payment order is pre-authorized;

30 Figure 13 is a block diagram of a typical network payment system in accordance with the invention;

Figure 14 is a flow chart illustrating the authentication, authorization, and settlement of a payment order;

- 8 -

Figure 15 is a flow chart illustrating an alternate processing of the authentication and verification of a payment order where transaction identifiers are used; and

5   Figure 16 is a flow chart illustrating an alternate processing of the authorization of a payment order where real-time approval from the financial authorization network may not be obtained.

DESCRIPTION OF A PARTICULAR PREFERRED EMBODIMENT

10   A network sales system 200 as shown in Figure 1 employs a network 67 to interconnect a plurality of buyer computers 61 and 62, merchant computers 63 and 64, each merchant computer with respective digital advertisement databases 65 and 66, and a payment computer 68. A user

15 of the system employs a buyer computer to retrieve advertisements from the merchant computers, and to purchase goods of interest. A payment computer is used to authorize a purchase transaction.

A digital advertisement includes a product

20 description and a price. In digital advertisement database 65 prices and descriptions may be stored separately, and one price may apply to many product descriptions.

In an alternate embodiment, the network sales

25 system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

The software architecture underlying the particular preferred embodiment is based upon the

30 hypertext conventions of the World Wide Web. Appendix A describes the Hypertext Markup Language (HTML) document format used to represent digital advertisements, Appendix B describes the HTML forms fill out support in Mosaic 2.0, Appendix C is a description of the Hypertext

35 Transfer Protocol (HTTP) between buyer and merchant

computers, and Appendix D describes how documents are
named with Uniform Resource Locators (URLs) in the
network of computers. A document is defined to be any
type of digital data broadly construed, such as
5   multimedia documents that include text, audio, and video,
and documents that contain programs.

Figure 2 shows an overview screen that has been
retrieved from a merchant computer by a buyer computer
and displayed by the buyer computer.   It includes links
10 1, 2, and 3 that when activated by a user cause the
buyer's computer to take specified actions. In the case
of link 1, the document shown in Figure 3 is retrieved
from a merchant computer and displayed. In the case of
link 2, a short audio segment is retrieved from a
15 merchant computer and played. In the case of link 3, the
query that can be entered into the query dialog box 4 is
sent to a merchant computer, and a document is retrieved
from the merchant computer and displayed.

Figure 3 shows a document that contains three
20 digital advertisements. The digital advertisements have
been retrieved from the merchant computer after the
activation of link 3. The merchant computer may set the
prices contained in the advertisements based on the on
the identity of the user as determined, for example, by
25 the network address of the requesting buyer computer.
The document includes links 5, 6, and 7 that are used to
purchase the products described by the advertisements.
For example, if link 5 is activated the missing payment
information document shown in Figure 4 is retrieved from
30 the merchant computer and displayed.

Figure 4 is a missing payment information
document that is used to gather user account information
for the requested purchase in an HTML form. Radio
buttons 8, 9, 10, 11, 12 are used to select a means of
35 payment, dialog box 13 is used to enter an account

- 10 -

number, dialog box 14 is used to enter an optional
authenticator for the account, purchase button 15 is used
to send the account information to the merchant computer
and proceed with the purchase, link 16 is used to abort
5   the purchase and return to the document shown in Figure
2, and dialog box 17 is used to enter optional user
information that is associated with the purchase and
ultimately used by a financial institution as part of a
textual billing identifier for the purchase transaction.
10 If provided, this additional information is included in
the payment order for the purchase.

Figure 5 is a fulfillment document 18 that is
produced once valid account information is provided to
the missing payment information document in Figure 4 and
15 purchase button 15 is activated.

Figure 6 is a flowchart that more fully describes
the information flow in the purchase transaction shown in
Figures 2 to 5. An initial user inquiry 19 from
activating link 1 results in the HTTP request 20 for a
20 specific document with a specified URL. The URL
specifies the name of the merchant computer.   The
merchant computer retrieves the document given the URL at
21, and returns it to the buyer computer at 22. The
buyer computer displays the resulting HTML document at
25 23. When the user activates link 5, an HTTP request 25
is sent to the merchant computer requesting the document.

In an alternate embodiment, document 22 is
executed at 23 as a program. A program is defined as a
set of instructions that can exhibit conditional behavior
30 based upon user actions or the environment of the buyer
computer. As is known to those skilled in the art, there
are many techniques for representing programs as data.
The program can be interpreted or it can be directly
executed by the buyer computer. The program when
35 executed will cause the buyer computer to interact with

- 11 -

the user leading to the user purchase request 24, and the purchase message 25.

The merchant computer then attempts to construct a payment order at 26 using the information it has
5 gathered about the user. The buyer computer may have previously supplied certain credentials using fill out forms or other account identification means such as providing the network address of the buyer computer in the normal course of communication. If the buyer
10 computer is able to construct a complete payment order at 26 the payment order is sent to a payment computer for authorization at 27. If a payment order can be constructed, processing continues at 28.

Alternatively, the buyer computer may construct
15 the payment order at 24 and send it to the merchant computer at 25. In this case, the payment order assembly steps at 26, at the merchant computer, may only need to forward the payment order from the buyer computer.

A payment order includes user account
20 information, merchant account information, an amount, and a nonce identifier that has not been previously used for the same user account. Variations of payment orders can be constructed, including payment orders that specify user or merchant identifiers in place of account
25 information, payment orders that specify a valid time period, payment orders that specify foreign currencies, and payment orders that include comment strings. Part of the process of constructing a payment order is creating a corresponding authenticator using one of the
30 authenticator methods described below.

In the illustrated embodiment of Figures 3 and 4, the merchant computer does not have sufficient information to construct a payment order at 26 and thus at 33 (Figure 7) constructs and returns a missing payment
35 information document in response to request 25.

- 12 -

Operation 33 includes in the constructed document
appropriate form fields based on what information the
merchant computer has already collected from the user.
The document is returned to the buyer computer at 34 and
5 is displayed at 35. When the user presses the purchase
button 15, the contents of the form are transmitted to
the merchant computer, at 36, to a specific URL name,
using an HTTP request. Based on the supplied form
fields, the merchant computer constructs a complete
10 payment order. Alternatively, the buyer computer may
construct the payment order at 35 and send it to the
merchant computer as part of step 36. In this case, the
payment order assembly steps 37 at the merchant computer
simply passes on the payment order from the buyer
15 computer. The payment order is sent to the payment
computer in a message at 38.

        In either case, the flowchart continues in Figure
6 where the payment computer checks the authorization of
the payment order at 28. If the payment system
20 authorizes the request, an authorization message at 29 is
returned to the buyer computer, and the merchant computer
checks at 30 that the authorization message came from the
payment computer using the authenticator mechanism
described below. Assuming that the authorization message
25 is valid, the merchant computer performs fulfillment at
30, returning the purchased product in response at 31.
In our example in Figure 5 the response at 31 is document
18 that was the logical target of link 5. If the payment
system does not authorize the payment order then response
30 31 is a rejection of the user's purchase request.

        In an alternate embodiment, step 30 can encrypt
the document using a key that is known to the buyer
computer. As is known to those skilled in the art, the
key can be communicated to the merchant computer using
35 convention key distribution protocols. In this manner

the document will be protected from disclosure to other
users.

The fulfillment step at 30 can alternatively
schedule a physical product to be shipped via ordinary
5   mail or other means. This can be accomplished by
updating a fulfillment request database or by sending a
message to a shipping system. In this case the response
at 31 is a confirmation that the product has been
scheduled to ship. In this way the network sales system
10 can implement an electronic mail order system.

Figures 8, 9, 10, and 11 show a second example
that uses query based access to digital advertisements.
It is assumed that the previous example was used by the
user immediately before at the same buyer computer.

15   Figure 8 shows the overview screen where the
query "movie review" has been entered into dialog box 39.
When the user activates process button 40, the merchant
searches databases as described by the URL attached to
button 40, and creates a response document as shown in
20 Figure 9.

Figure 9 shows digital advertisements 39, 40, 41,
42, 43, and 44 that were found in response to the query
initiated by button 40. A scroll bar 45 shows that there
are additional digital advertisements that are not shown.
25 When link 46 is activated, the missing account
information document shown in Figure 10 is returned by
the merchant computer.

Figure 10 shows that the merchant computer has
partial information on the buyer's account. Message 47
30 shows that the merchant computer already knows the
buyer's account number. Purchase button 48 will send the
optional user reference string in dialog box 50 to the
merchant computer described by the URL behind button 48
and purchase the product corresponding to digital

- 14 -

advertisement 39.   Cancel link 49 will return the user to
the document shown in Figure 2.

When purchase button 48 is activated, a document
51 is sent by the merchant computer and displayed by the
5 buyer computer as shown in Figure 11.

Figure 12 shows an alternative method of·
processing a sales transaction.   In this method when the
user requests a purchase at 52, the buyer computer
constructs a payment order at 53 and sends it for
10 approval to the payment computer at 54.   The payment
computer authorizes the payment order at 55; and when the
payment order is authorized, returns an unforgable
certificate at 56 that the payment order is valid.   Means
of creating such unforgable certificates are described in
15 authenticator method number one below.   If at step 55 the
payment order is not authorized, a rejection message is
sent at 56 and the sales transaction is terminated.

The buyer computer then proceeds at 57 to send a
pre-authorized purchase request to the merchant computer.
20 The unforgable certificate 56 is included in a purchase
message at 57 that is sent at 58 to the merchant
computer.   Based upon the pre-authorized payment order
the merchant computer performs fulfillment at 59 and
returns the product at 60.   In a variation, the merchant
25 computer at 59 checks to ensure the payment order has not
been previously used.   This can be accomplished by
checking with a payment computer or maintaining a
merchant computer database of previously accepted payment
orders.   The unforgable certificate created at step 56
30 does not need to include the user account information.
This variation is useful if the user wishes to make
purchases and remain anonymous to the merchant.

- 15 -

A Network Payment System

        A network payment system 300 as shown in Figure
13, employs a public packet-switched network 69 to
interconnect a plurality of client computers 70 and 71,
5 and a plurality of payment computers such as 72, each
payment computer having an account database 73, a
settlement database 74, an authorized address database
75, a sender credential database 76, a financial system
interface 77, and a real-time authorization interface 78.
10 The interfaces 77 and 78 may be implemented by a single
communications line.

        In an alternate embodiment, the network payment
system further includes external devices that are kept in
the possession of users so that the users can
15 authenticate themselves when they use a buyer computer.

        Account database 73 maintains temporal spending
amounts, such as the amount spent in the current day, and
also maintains temporal spending limits. The account
database may also maintain a translation between
20 principal identifiers and external account identifiers.
Settlement database 74 records committed payment orders
along with any authorization information for the orders
that was obtained from interface 78. Address database 75
maintains for each sender a list of authorized buyer
25 computer and delivery addresses. Credential database 76
maintains a list of credentials for principals and
information that can be used to authenticate principals.

        Figure 14 is a flowchart that describes the
operation of the payment system. A client computer 71
30 constructs a payment order at 79, and computes and adds
an authenticator to the payment order at 80. The payment
order is sent at 81 to a payment computer, where the
authenticator is verified at 82 to ensure that the
payment order was originated by the sender it describes.

- 16 -

Below we present different means of implementing 80 and
82.

If the payment order is authentic and address
restrictions are desired, at 83, either or both of the
5   client computer address or the specified delivery address
can be checked against address database 75. If address
restrictions are desired and if the addresses in the
payment order are not in the database, the payment
computer sends a rejection message to the client
10 computer. Address database 75 specifies, for each
principal, acceptable client computer addresses and
delivery addresses. A delivery address can be a network
address, or a street address for packaged goods. As is
known in the art, database 75 can include wild-card
15 specifications and similar techniques to reduce its size.

For example, database 75 could contain an entry for
principal identifier "*@acme.com" restricting legal
delivery addresses to "computer: *.com", "computer:
cmu.edu", and "surface: *, 34 Main Street, Anytown, USA",
20 indicating that any user at the company Acme can order
products to be delivered to the network address at Acme
or the university CMU, or to anyone at 34 Main Street,
Anytown, USA.

If payment order address restrictions are not
25 desired or have been checked, processing continues at 84
where the payment order is checked for replay and
temporal spending limits. Replay is checked for by
making sure that the sender did not previously present a
payment order with the same nonce by checking an index of
30 committed payment orders by nonce in settlement database
74. If nonces are based on time, then a payment order
that is older than an administratively determined value
can be rejected out of hand. Time based nonces or
sequential nonces permit old nonces to be removed from
35 the settlement database 74. If a payment order has been

- 17 -

previously processed or its nonce is too old, the payment
order computer sends a rejection message to the client.

After the payment order passes the replay check,
temporal spending limits are checked in account database
5   73. These spending limits can be applied on a per
sender, per group of senders, and per payment system
basis to limit fraud risk. The limits can be applied to
any duration of time, for example a maximum spending
amount per hour or per day. If the payment order would
10 violate a spending limit, the payment computer sends a
rejection message to the client.

Once the payment order passes the temporal
spending check at 84, a message is constructed at 85 to
check that the external account that backs the sender's
15 payment system account has adequate funds or credit. If
the sender identifier in the payment order is not already
an account number in the external financial system, it is
translated into a corresponding account number in the
external financial system using account database 73. A
20 real-time authorization request message is sent at 86 to
the external financial system over interface 78. If the
external financial system approves authorization request
86, an authorization message is returned at 87. If
request 86 is not approved, the payment computer sends a
25 rejection message to the client at 87.

In a variation of the above described approach,
processing continues at 95 after 84. At 95 real-time
authorization is only obtained when the total of a
sender's payments since the last real-time authorization
30 reaches a preset value, or the payment order is over a
preset amount. These preset values can be optionally
recorded on a per principal basis in database 73 or can
be administratively determined for all principals. In
this manner, the number of messages to the external
35 financial system can be reduced. In addition, the

- 18 -

payment system can avoid making real-time authorization
requests for small payments when the risk is acceptable
to the payment system operator. If real-time
authorization is necessary, processing continues at 85
5 after 95. If real-time authorization is not necessary
for a request, at 100 the payment order amount is added
to the sender's total of payments since the last real-
time authorization in database 73, and processing
continues at 88.

10   In another variation after 100 a check is made at
101 in database 73 to see if a background authorization
process should be scheduled. A background authorization
process permits the payment computer to continue its
normal processing while it checks with the financial
15 authorization network on the sender's account. This
mechanism can be used to limit payment system risk. If
the background authorization fails, the account is
suspended by so updating database 73. If the sender's
total of payments since last authorization is over a
20 preset value stored in 73 then a background authorization
process is scheduled at 102. Otherwise processing
continues at 88.

        In another variation, at 95 and 101
authorizations are obtained based on the amount spent
25 since last authorization and time since last
authorization.

        At 88 the payment order is committed to execution
and is recorded in settlement database 74. Recorded with
the payment order in database 74 are portions of
30 authentication message 87 that show that the payment
computer contacted the remote financial system. The
amount of the payment order is added to running temporal
spending records in database 73, and an authorization
message is sent to the client computer at 90. The
35 authorization message includes the payment order. In an

- 19 -

alternate embodiment, at 90 the authorization message
contains a truncated payment order that includes at least
the payment order's sender and the payment order's unique
nonce.

5   In an alternate embodiment, the authorization
message sent to the client at 90 includes at least one
legal delivery addresses for the sender as determined
from database 75.

           Authorization message 90 must be transmitted in
10 such a way that the client computer can be sure that it
came from the payment computer. At 89 a payment system
specific authenticator is added payment order. At 91
this authenticator is checked by the client computer.
The steps at 89 are a dual of step 80, and the steps at
15 91 are a dual of step 82. The authentication means for
steps 89 and 91 are described below.

           Finally, settlement is performed at 92 in the
external financial system 77 between external accounts
that correspond to the sender and the beneficiary. If
20 settlement is accomplished as part of real-time
authorization at steps 86 and 87, as may occur in a real-
time debit network, then no other steps need to be taken.
If settlement is not accomplished as part of the
authorization process, then financial system messages are
25 sent to interface 77 to effect settlement. Depending on
the external accounts involved, these messages may
include electronic funds transfer messages or automated
clearinghouse messages.

           In an alternate embodiment, at 92 settlement
30 messages are sent to reconcile net transfer balances
between principles on a temporal basis, for example once
a day. In this embodiment the number of settlement
messages can be less than the number of payment orders.

           Authenticators may be created and checked using
35 one of the following methods. The payment computer can

- 20 -

use any of the first four methods, and the client
computer can use any of the methods described.

In a first method for authenticators, at steps 80
or 89, a digest of the payment order is signed by the
5 sending computer using a public-key cryptographic system
such as RSA. This signature is used as the
authenticator. As is well known in the art, the signing
can be accomplished using a private key created from a
public-key pair, where the signing key is only known by
10 the signer, and the other public key is known to the
receiving computer. At the payment computer the public
key corresponding to each sender is kept in credential
database 76. The private key for the payment service is
also kept in database 76. At steps 82 or 91, the
15 signature of the received message is checked using the
public key known to the receiving computer.

In a second method for authenticators, at steps
80 or 89, a digest of the payment order is signed by the
sending computer with a private key cryptosystem such as
20 DES. This signature is used as the authenticator. At
the payment computer, the private key corresponding to
each sender is kept in credential database 76. At step
80, a digest of the payment order is signed by the client
computer, and at step 89 a digest of the payment order
25 with an added approval code is signed by the payment
computer using the same private key. At steps 82 or 91,
the signature of the received message is checked using
the shared private key.

In a third method for authenticators, at step 80
30 the authenticator is computed by a protected device
external to the system such as a Smart-Card. A protected
device is specifically designed to be extremely difficult
both to replicate and to compromise. In this method, the
payment order is communicated at 80 to a Smart-Card. The
35 Smart-Card computes and signs a digest of the payment

- 21 -

order, and then communicates the signature back at 80 to
be used as an authenticator. A Smart-Card produced
authenticator uniquely associates a payment order with
its creating Smart-Card. This is accomplished by having
5 the Smart-Card contain a secret key "K" that is used to
create a digital signature of the payment order. "K" is
never released outside of the Smart-card. The Smart-Card
is designed to make it computationally infeasible to
compute "K" even with possession of the device. In this
10 method, at step 82, a signature checking key from
database 76 is used to check the authenticator. In an
alternate embodiment, a user must manually signal their
acceptance of each payment order on an input device that
is part of the external device before the authenticator
15 is created by the external device.

In a fourth method for authenticators, at steps
80 or 89, a network address is used as an authenticator.
At steps 82 or 91, a digest of the payment order is sent
back to the specified network address along with a random
20 password. The computer at the specified network address
must then return the payment order digest along with the
password. If the network guarantees to deliver messages
to the proper network address, this method will guarantee
that the user or computer at the specified network
25 address approves of the payment order. Assuming that
network delivery is trusted, this method can be used to
authenticate a sender computer's network address in a
payment order. Alternatively, electronic mail can be
used to send such confirmation messages between a user
30 and the payment system.

In a fifth method for authenticators, at step 80,
the authenticator is produced by an external device that
produces a sequence of non-predicable transaction
identifiers that are device specific. The authenticator
35 is entered by the user into the client computer by

- 22 -

reading its display. One such device is described in
U.S. Patent 4,856,062. According to this method, at step
91, the authenticator can be checked using the sender
specific fixed code of the device which is kept in
5 database 76. This sequence of steps is also shown in
Figure 15 at steps 93 and 94.

In a sixth method for authenticators, at step 80,
the authenticator is obtained by querying the user for a
transaction identifier that is the next string from a
10 physical list of one-time authorization strings. Such as
list could be produced on a card, and the user can cross
off authorization strings as they are used. According to
this method, at step 91, the authenticator is checked
against the next expected string from the sender using
15 database 76. Database 76 can hold for each sender a list
of random authorization strings, or can hold a sender
specific secret key that was used to generate the list of
authentication strings along with how many strings have
been used so far. This sequence of steps is also shown
20 in Figure 15 at 93 and 94.

In a seventh method for authenticators, at step
80 the authenticator is a previously obtained personal
identification number (PIN) for the user. In this method
in 91 the authenticator is checked against the expected
25 PIN for the sender using database 76.

As will be obvious to one skilled in the art, any
of the methods for creating authenticators can be used
together to increase system security. For example,
authenticator method six can be used to create an
30 authenticator based on a transaction identifier, and then
a payment order including a transaction identifier can be
given a further authenticator using authenticator method
one. In this example the resulting authenticators would
be checked with their respective methods.

- 23 -

A digest of a payment order can be created with
an algorithm such as MD5 [R. Rivest, The MD5 Message-
Digest Algorithm, MIT Laboratory for Computer Science,
Network Working Group Request for Comments 1321].
5 Alternatively, a digest can be the entire payment order
or other functions of the payment order's component
parts.

In addition in both the sales and payment systems
alternate authenticator techniques can be used such as
10 those described by Voydock and Kent in "Security
Mechanisms in High-level Network Protocols", Computing
Surveys Vol. 15, No. 2, June 1983. As will be
appreciated by those skilled in the art, two-way
authenticated byte-stream or remote procedure call
15 interface connections that protect against replay can
replace our message based authenticators.

Additions, subtractions, deletions, and other
modifications of the described embodiment will be
apparent to those practiced in the art and are within the
20 scope of the following claims.

- 24 -

CLAIMS

1. A network sales system comprising

    a plurality of buyer computers and at least one merchant computer interconnected by a communications network,

5   means at each merchant computer for maintaining and providing a database of digital advertisements comprising

        means for storing said digital advertisements, each digital advertisement including a product abstract,

10   means for communicating a digital advertisement to a buyer computer over said network in response to a network request from said buyer computer,

        means at each buyer computer for requesting, displaying, and responding to digital advertisements

15 comprising

        means responsive to a user inquiry for selecting a merchant computer and obtaining a digital advertisement for a product from said database of advertisements at said merchant computer,

20   display means for displaying said advertisement,

        purchase means responsive to a user request for communicating a purchase message to said merchant computer,

        account identification means for transmitting the

25 user's account information to said merchant computer,

        means, at said merchant computer, comprising

        authorization means to authorize said purchase message by sending messages into a financial system network,

30   fulfillment means to send said product to user conditional on approval of said authorization means.

- 25 -

2. The network sales system of claim 1 further wherein said authorization means at said merchant computer comprises

means for communicating a missing payment
5 information request message to said buyer computer to obtain missing payment information,

means for receiving said missing payment information from said buyer computer,

means for authorizing said purchase message by
10 sending messages into a financial system network,

and said account identification means at said buyer computer comprises

means responsive to said missing payment information request message to query the user for
15 additional payment information,

means to send said additional payment information to said merchant computer.

3. The network sales system of claim 1 further wherein said account identification means comprises
20   means for assembling a payment order,

means for sending said payment order to a network payment system for authorization,

and wherein said authorization means comprises

means for verifying that said payment order has
25 been previously authorized by said payment system.

4. An electronic sales system comprising

means for storing a database of digital advertisements, each digital advertisement for a product including a program,
30   means for communicating a digital advertisement to a buyer computer,

means at said buyer computer for displaying and responding to said digital advertisement comprising

- 26 -

display means for displaying said digital
advertisement by executing a portion of said
advertisement as a program and performing actions as
specified by said program,

5   purchase means responsive to a user request for
communicating a purchase message to a merchant computer,
          means, at said merchant computer, comprising
          fulfillment means to send said product to user.

          5. A network payment system comprising
10   a plurality of client computers and at least one
payment computer interconnected by a public packet
switched communications network,
          means at a client computer for performing payment
comprising
15   payment specification means for
constructing a payment order from a sender to a
beneficiary,
                   signing means for authenticating said
payment order as originating from said sender,
20   means for sending said payment order to a payment
computer,
          means for receiving a payment order authorization
message from said payment computer,
          means responsive to a payment order message at
25 said payment computer comprising
                   verification means for verifying that said sender
originated said payment order,
authorization means for sending a message into a
financial authorization network to verify that said
30 sender has adequate funds or credit and receiving an
authorization in response,
                   means for recording said payment order and
authorization in a settlement database,

- 27 -

     response means for sending an
authorization message to said client computer,
     means for sending at least one message
into a financial system network to transfer funds from
5 said sender to said beneficiary.

     6. The network payment system of claim 5 further
wherein said payment specification means comprises
     means for constructing a payment order, said
payment order including a delivery address,
10   and said verification means comprises
     means for verifying that said sender originated
said payment order and checking said delivery address
against a database of allowed delivery addresses for said
sender.

15   7. The network payment system of claim 5 further
wherein said response means comprises
     means for determining allowed delivery addresses
for said sender,
     means for sending an authorization message to
20 said client computer that includes allowed delivery
addresses.

     8. The network payment system of claim 5 further
wherein said signing means comprises
     means for generating the next expected
25 transaction identifier for said sender and using it to
create an authenticator,
     and wherein said verification means comprises
     means for generating the next expected
transaction identifier for said sender, and
30   means for verifying that said authenticator was
created using said transaction identifier.

- 28 -

9. The network payment system of claim 5 further wherein said signing means comprises

means for generating an authenticator using an external device,

5   and wherein said verification means comprises

means for verifying that said authenticator was created using said external device.

10. The network payment system of claim 5 further wherein said payment specification means

10 comprises

means for constructing a payment order from a sender, said payment order including a client computer's network address,

and said verification means comprises

15   means for verifying said payment order was constructed at said client computer's network address and checking said client address against a database of allowed client addresses for said sender.

11. The network payment system of claim 5

20 further wherein said authorization means comprises

determination means for determining the necessity for real-time authorization,

means for performing real-time authorization conditioned on said determination means.

25   12. A method for effecting sales over a network sales system having a plurality of buyer computers and at least one merchant computer interconnected by a communications network, encompassing the steps of

maintaining and providing a database of digital

30 advertisements at each merchant computer

storing said digital advertisements, each digital advertisement including a product abstract,

- 29 -

communicating a digital advertisement to a buyer
computer over said network in response to a network
request from said buyer computer,
            requesting, displaying, and responding at each
5 buyer computer to digital advertisements comprising the
steps of
            selecting in response to a user inquiry a
merchant computer and obtaining a digital advertisement
for a product from said database of advertisements at
10 said merchant computer,
            displaying said advertisement,
            communicating in response to a user request a
purchase message to said merchant computer,
            transmitting the user's account information to
15 said merchant computer,
            authorizing at said merchant computer said
purchase message by sending messages into a financial
system network, and
            sending said product to said user conditional on
20 approval from said authorizing step.

            13.   The network sales method of claim 12 further
wherein said authorizing step, at said merchant computer,
comprises the steps of
            communicating a missing payment information
25 request message to said buyer computer to obtain missing
payment information,
            receiving said missing payment information from
said buyer computer,
            authorizing said purchase message by sending
30 messages into a financial system network,
            and said account identification step at said
buyer computer comprising the steps of

- 30 -

querying the user for additional payment
information responsive to said missing payment
information request message,
        and sending said additional payment information
5 to said merchant computer.

        14.   The network sales method of claim 12 further
wherein said account identification step comprises the
steps of
        assembling a payment order, and
10   sending said payment order to a network payment
system for authorization,
        and wherein said authorization step comprises the
step of
        verifying that said payment order has been
15 previously authorized by said payment system.

        15.   An electronic sales method comprising the
steps of
        storing a database of digital advertisements,
each digital advertisement for a product including a
20 program,
        communicating a digital advertisement to a buyer
computer,
        displaying and responding to said digital
advertisement at said buyer computer comprising the steps
25 of
        displaying said digital advertisement by
executing a portion of said advertisement as a program
and performing actions as specified by said program,
        communicating a purchase message in response to a user
30 request to a merchant computer,
        sending at said merchant computer said product to
user.

- 31 -

16.   A network payment method comprising the
steps of interconnecting a plurality of client computers
and at least one payment computer by a public packet
switched communications network,

5   performing payment at a client computer
comprising the steps of
            constructing a payment order from a sender to a
beneficiary,
            authenticating said payment order as originating
10 from said sender,
            sending said payment order to a payment computer,
            and receiving a payment order authorization
message from said payment computer,
            responding to a payment order message at said
15 payment computer comprising the steps of
            verifying that said sender originated said
payment order,
            sending a message into a financial authorization
network to verify that said sender has adequate funds or
20 credit and receiving an authorization in response,
            recording said payment order and authorization in
a settlement database,
            sending an authorization message to said client
computer,
25   and sending at least one message into a financial
system network to transfer funds from said sender to said
beneficiary.

17.   The network payment system of claim 16
further wherein said constructing step means comprises
30 the steps of
            constructing a payment order, said payment order
including a delivery address,
            and said verifying step comprises the steps of

- 32 -

    verifying that said sender originated said
payment order, and
    checking said delivery address against a database
of allowed delivery addresses for said sender.

5   18.   The network payment method of claim 16
further wherein said second sending step comprises the
steps of
    determining allowed delivery addresses for said
sender,
10   and sending an authorization message to said
client   computer that includes allowed delivery
addresses.

    19.   The network payment method of claim 16
further wherein said authenticating step comprises the
15 steps of
    generating the next expected transaction
identifier for said sender and using it to create an
authenticator,
    and wherein said verifying step comprises the
20 steps of
    generating the next expected transaction
identifier for said sender,
    and verifying that said authenticator was created
using said transaction identifier.

25   20.   The network payment method of claim 16
further wherein said authentication step comprises the
step of
    generating an authenticator using an external
device,
30   and wherein said verifying step comprises the
steps of

- 33 -

verifying that said authenticator was created using said external device.

21. The network payment method of claim 16 further wherein said constructing step comprises the step
5   of

constructing a payment order from a sender, said payment order including a client computer's network address,

and said verifying step means comprises the steps
10 of

verifying said payment order was constructed at said client computer's network address,

and checking said client address against a database of allowed client addresses for said sender.

15   22. The network payment method of claim 16 further wherein said second sending step comprises the steps of

determining the necessity for real-time authorization,

20   and performing real-time authorization conditioned on its determined necessity.

1/16

FIG. 1

NCSA Mosaic: Document View

File   Options   Navigate   Annotate   Help

Document Title: | Welcome to The Information Exchange |

Document URL: | http://sparta.lcs.mit.edu/gifford/ix-1.html |

Times

Welcome to The Information Exchange

Today's Headlines —1

Radio Headlines —2

Query:

Process

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 2
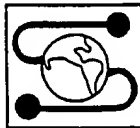
NCSA Mosaic: Document View

File   <u>O</u>*ptions*   <u>Na</u>*vigate*   <u>A</u>*nnotate*   <u>He</u>*lp*

Document Title: The Information Exchange eadlines

Document URL: http://sparta.lcs.mit.edu/gifford/ix-2.htal

New York Times Headlines

SHUTTLE HUBBLE (Houston)- Arriving for a house call 357 miles above Earth, the
astronauts of the space shuttle Endeavor on Saturday reached out with a
mechanical grappling arm and easily snared the Hubble space telescope and
prepared to treat the crippled spacecraft in five days of the most
complex orbital repairs yet attempted.
By John Noble Wilford

<u>$1.00</u>   <u>5</u>

HEALTH-ALLIANCE (Washington)- If the Clinton health plan becomes law, ti will put
a new institution into the lives of most Americans: the health alliance. Almost
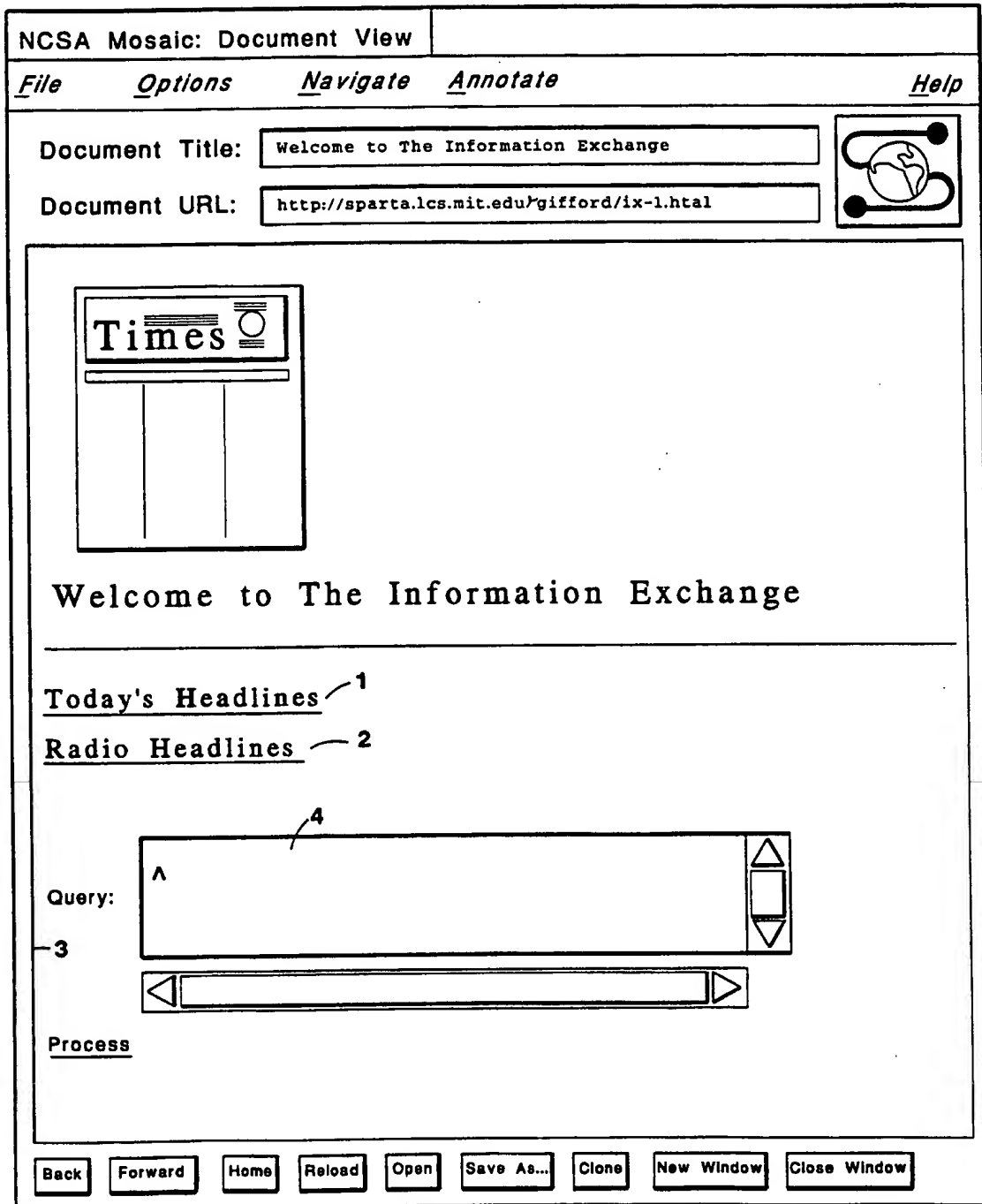no other aspect of the plan is so little understood or so radically different
from the status quo. By Robin Toner.

<u>$0.75</u>   <u>6</u>

GAMBLING (Las Vegas)- The newest perspective on the booming national industry
of legalized gambling is now open for business: futuristic virtual-reality
rides to soothe the losers' souls, just up the theme park escalator from
acres of the latest video slot machines. By Francis X. Clines.

<u>$0.75</u>   <u>7</u>

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 3

FIG. 4

18

NCSA Mosaic: Document View

File   *Options*   *Navigate*   *Annotate*   *Help*

Document Title: TROUBLED HUBBLE SPACE TELESCOPE PULLED IN BY SHUTTLE FOR REPAIRS

Document URL: http://sparta.lcs.mit.edu/gifford/ix-7.html

TROUBLED HUBBLE SPACE TELESCOPE PULLED IN BY SHUTTLE FOR REPAIRS

By JOHN NOBLE WILFORD
The New York Times (Copyright 1993 The New York Times)

priority: Urgent
date: 12-04-93 1712EST
catagory: Domestic
subject: BC SHUTTLE HUBBLE ART

HOUSTON- Arriving for a house call at 357 miles above Earth,the astronauts
of the space shuttle Endeavor reached out Saturday with a mechanical
grappling arm and easily snared the Hubble telescope.

The orbital retrieval paves the way for the shuttle's astronauts to treat
the crippledspacecraft in five days of the most complex orbital repairs
yet attempted.

"Houston, Endeavorhas afirm handshake with mr. Hubble's telescope," Col.
Richard D. Coveyof the Air Force, the shuttle commander, radioed to
Mission Control in Houston after the robotic arm had grasped the 1.6
billion telescope.

The shuttle's successful rendezvous with the orbiting telescope was the
first major step in a mission that could be fateful to both astronomy and
NASA

Installing new mirrors to overcome Hubble's blurred visionwill return the
telescope to its full abilities, giving the astronomers a view almost to
the edge of the universe. And such a highly visible success could boost
the space agency's reputation at a time it is seeking support for building
an international space station

Once the 12.5-ton telescope was securely berthed in the oper cargo bay
Saturday morning, it was ready for the astronauts to begin the first of
their five space walks early Sunday morning

The schedule calls for Dr. Musgrave and Dr. Jeffrey A. Hoffman to replace
failed gyroscopes, two electronic control units and some fuses.

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 5

**BUYER
COMPUTER**   **MERCHANT
COMPUTER**   **PAYMENT
COMPUTER**

19 ⌐ User   Inquiry

20 ⌐| Request   Advertisement(s)
→

                                                      Retrieve   Digital ⌐ 21
                                                      Advertisement(s)
              22
             /
    Digital Advertisement(s) |
←

    |

Display   Digital ⌐ 23
Advertisment

    |

User Requests ⌐ 24
Purchase

    | 25
                  /
    · Purchase   Message
→

                      | Construct Payment
                      26
                     /
                      Construct Payment
                      Order   27
                      | Payment Order /
                      →

                                            | 28
                                                      /.
                                            Authorize Purchase

                                  Authorization   Message |
                                  ←
                                                          \
                                                          29

                      |

              31   Perform Fullfillment
)   \
      Product | 30
←

FIG. 6

7/16

BUYER   MERCHANT   PAYMENT
COMPUTER   COMPUTER   COMPUTER

Purchase   32
Message

                        Construct Missing Payment   33
                        Information Request

        Missing Payment
        Information Req.
                        34

Query User for   35
Payment Information

        Missing Payment /   36
        Information Message

                        Construct Payment   37
                        Order

                        Payment Order   38

FIG. 7

NCSA Mosaic: Document View

File   *Options*   *Navigate* *Annotate*   *Help*

Document Title: | Welcome to The Information Exchange |

Document URL: | http://sparta.lcs.mit.edu/gifford/ix-1.htal |

Times ☑

Welcome to The Information Exchange

Today's Headlines

Radio Headlines

39

movie review

Query:

Process ⟋ **40**

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 8

NCSA Mosaic: Document View

File   *Options*   *Navigate*   *Annotate*   *Help*

Document Title: Query Results: movie review

Document URL: http://sparta.lcs.mit.edu/gifford/ix-4.html

QUERY RESULTS: movie review

1. Dec. 2 1993 14;32 [78 lines] $1.00 —46   **39**   45

In "A Dangerous Women," Debra Winger sinks deeply into the drab role of Martha Horgan, a sheltered innocent living in a small California town.

2. Dec. 2 1993 14:23 [60 lines] $1.00   **40**

"Deception" is a fabulously.farfetched story about the string of suprises that leads Bessie Faro (Andie MacDowell) all over the world.

3. Nov. 26 1993 19:43 [49 lines] $1.00   **41**

"Twenty Bucks" follows a $20 dollar bill from the moment it's dispensed by an automatic teller machine to its destruction months later. Along the way it passes through the hands of dozens of individuals from all walks of life.

4. Nov. 23 1993 18;46 [48 lines] $1.00   **42**

(" A Perfect World," a drama, is rated PG-13 for language and violence. It received 3 and one-half stars out of 4.)
Clint Eastwood and Kevin Costner represent the best of Hollywood's stars who entertain without sacrificing artistic integrity. In "A Perfect World," their reputations remain intact.

5. Nov. 23 1993 18:46 [53 lines] $1.00   **43**

("GEORGE BALANCHINE'S 'NUTCRACKER," a dance film, is rated G. It received 2. stars out of 4.)
A straightforward record of the annual Christmas show staged by the New York City Ballet, "George Balanchine's 'Nutcracker,'" would have gone directly to TV if not for the participation of

6. Nov. 23 1993 18:46 [60 lines] $1.00   **44**

("WE'RE BACK! A DINOSAUR'S STORY," an animated feature, is rated G. It received 2 stars out of 4.)
Kids won't even understand the best joke in the animated "We're Back! A Dinosaur's Story." It has to do with a godlike line- and space-traveling

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 9

NCSA Mosaic: Document View

File   *Options*   *Navigate*   *Annotate*   *Help*

Document Title: | Confirm Charge |

Document URL: | http://sparta.lcs.mit.edu/gifford/ix-5.htal |

Digital Copyright License Purchase

In exchange for the specified fee you will be licensed for individual use of the copyrighted material

Confirm a charge of $1.00 ov your VISA 4262 1501 2000 1466 — **47**

Purchase —**48**

Cancel —**49**

Your Reference:

50

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 10

51

NCSA Mosaic: Document View	

| _File_ | _Options_ | _Navigate_ | _Annotate_ | _Help_ |

Document Title: | A DANGEROUS WOMAN

Document URL: | http://sparta.lcs.mit.edu/gifford/ix-6.html

A DANGEROUS WOMAN

By JANET MASLIN

The New York Times (Copyright 1993 The new York Times

priority: Regular
date: 12-02-93 1432EST
catagory: Entertainment and Culture
subject: BC WOMEN FILM REVIEW

In "A Dangerous Women," Debra Winger sinks deeply inti the drab role of
Martha Horgan, a shelteredinnocent living in a small California town.

Characters like martha have a way attracting the storyteller's interst at a
very precise point in their lives. It is the moment just before the
character's peaceful existence is ruptured by some seismic force like sex
or death or a symbolic coming of age.

"A Dangerous Women" is soap opera enough to churn up all three.

With Ms. Winger's eerily convincing performance at it's centerpiece, the film
creates a world of sexual chicanery that would do any television series
proud.

Martha is taken care of by aunt Frances (Barbara Hershey), a rich, beautiful
widow involved in an extramarital affair with a state assemblyman
(John Terry). That liaisonstarts off the film with a suitable bang, as the
assembly's wife (laurie metcalf) drunkenly drives her car into the widow's
front porch as a means of registering her irritation.

Martha, a fragile creature in a girlish nightgown and thick glasses,
watches this outburst in bewildered horror. But the film intends it as a
harbringer of Martha's own act of violence, which is already in the
works and will serve as

| Back | Forward | Home | Reload | Open | Save As... | Clone | New Window | Close Window |

FIG. 11

12/16

| BUYER | MERCHANT | PAYMENT |
| COMPUTER | COMPUTER | COMPUTER |

User Requests ╱52
Purchase

Construct Payment ╱53
Order

54
Payment Order →

55
Authorize Payment Order

Authorization Message
←
56

Construct ╱57
Purchase Mesage
with Authorized
Payment Order

Purchase Message ╱58
→

Perform Fullfillment ──59

Product
←
60

FIG. 12

FIG. 13

14/16

CLIENT COMPUTER	PAYMENT COMPUTER	REAL-TIME FINANCIAL AUTHORIZATION NETWORK

79 — Construct Payment Order

80 — Compute and Add Authenticator

81

Payment Order

82 — Verify Authenticator

83 — Check for Address Restrictions

84 — Check for Replay and Spending Limits

85 — Construct Message for Real-Time Authorization

86

Authorization Request

Authorization Number

87

Record Payment Transaction — 88

90

Add Authenticator to Authorization Message — 89

Authorization Message

Verify Authorization Authenticator

91

Perform Settlement   92

FIG. 14

15/16

| CLIENT COMPUTER | PAYMENT COMPUTER | REAL-TIME FINANCIAL AUTHORIZATION NETWORK |

Construct Payment Order

Add Tranasction Identifer as part of Authenticator — 93

Payment Order →

Verify Authenticator and Confirm Transaction Identifer is One Expected — 94

FIG. 15

PAYMENT   REAL-TIME
COMPUTER   FINANCIAL
                                           AUTHORIZATION
                                           NETWORK

Check for Replay and Spending Limits

Real-Time   Authorization   Necessary? — **95**

| No ⁄**100** | Yes

Update Account Database   Construct Message for — **96**
                              Real-Time Authorization
| ⁄**101**   **97**
Schedule Background | Authorization Request
Authorization?

| Yes   └No   Authorization Number ⫶
Request Background   ⟵————————————
Authorization   **98**
⁄ └——————————
102

                    Record Payment Transaction—— **99**

FIG. 16

A.   CLASSIFICATION OF SUBJECT MATTER

IPC(6)   :G06F 157:00

US CL   :364/401,408

According to International Patent Classification (IPC) or to both national classification and IPC

B.   FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/401, 406, 408; 340/825.33; 380/23, 24; 902/1, 2, 24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS Database Search

Search terms include: home(2a)shop?, electronic?(2a)shop?, advertis?(p)program, download?(w)program?

C.   DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,799,156 (SHAVIT ET AL.) 17 January 1989, see entire document.	1-22
Y	US, A, 4,992,940 (DWORKIN) 12 February 1991, see col. 2, lines 30-34.	1-22
Y	US, A, 4,775,935 (YOURICK) 4 October 1988, see figures 5b and 6.	4, 15
Y	US, A, 4,935,870 (BURK, JR. ET AL.) 19 June 1990, see col. 15.	4, 15
Y	US, A, 5,025,373 (KEYSER, JR. ET AL.) 18 June 1991, see col. 4, lines 45-58, col. 6, lines 1-25, and col. 8, lines 39-45.	5, 8-9, 16, 19-20

[X] Further documents are listed in the continuation of Box C.   [ ]   See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 JANUARY 1995	**01 MAY 1995**

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	DAVID M. HUNTLEY
Facsimile No. (703) 305-3230	Telephone No. (703) 305-9775

Form PCT/ISA/210 (second sheet)(July 1992)*

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

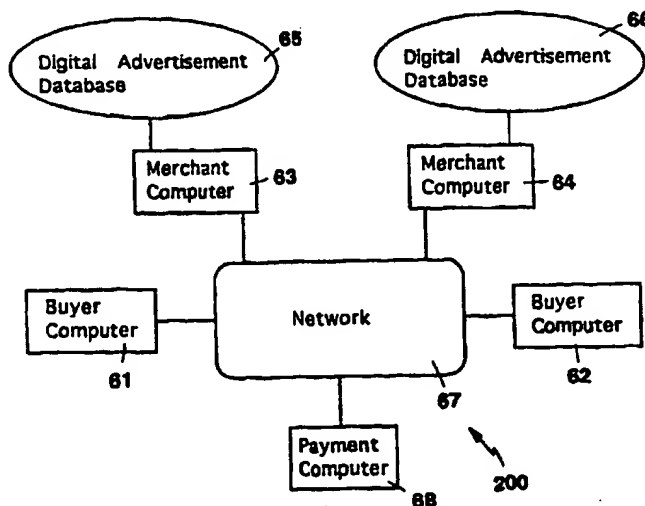| Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,812,628 (BOSTON ET AL.) 14 March 1989, see entire disclosure.	11, 22
Y	US, A, 4,922,521 (KRIKKE ET AL.) 01 May 1990, see col. 6, lines 1-52.	6-7, 10, 17-18, 21

(54) Title: DIGITAL ACTIVE ADVERTISING

(57) Abstract

A complete system (200) for the purchasing of goods or information over a computer network (67) is presented. Merchant computers (63, 64) on the network (67) maintain databases of digital advertisements (65, 66) that are accessed by buyer computers (61, 62). In response to user inquiries, buyer computers (61, 62) retrieve and display advertisements from merchant computers (63, 64). A digital advertisement can include a program that is interpreted by a buyer's computer (61, 62). The buyer computers (61, 62) allow the users to purchase the product described by an advertisement. The form of payment can be requested after a purchase is initiated. A payment system (300) performs payment authorization. The payment system obtains account authorizations from an external financial system. Payment orders are signed with authenticators.

AMENDED CLAIMS
[received by the International Bureau on 3 July 1995 (03.07.95);
original claims 1-22 replaced by amended claims 1-42 (13 pages)]

```
1          1.   A network sales system providing for real-time
2   authorization of purchase transactions, comprising:
3               a plurality of buyer computers; and
4               a plurality of merchant computers;
5               said plurality of buyer computers and said
6   plurality of merchant computers being interconnected by a
7   public packet switched communications network;
8               at least one of said plurality of merchant
9   computers being programmed to store digital
10  advertisements in a database;
11              each one of said buyer computers being programmed
12  to receive a user inquiry and, in response to said user
13  inquiry, to select at least one of said merchant
14  computers and to transmit a network request thereto;
15              at least one of said merchant computers being
16  programmed to cause one of said digital advertisements to
17  be communicated to said one of said buyer computers over
18  said public packet switched communications network in
19  response to said network request from said buyer
20  computer;
21              said one of said buyer computers being programmed
22  to display said one of said digital advertisements, and,
23  in response to a user request, to transmit to at least
24  one of said merchant computers a purchase message and to
25  cause a payment request, comprising a payment amount, to
26  be transmitted into a payment system in order to initiate
27  authorization of purchase of a product having real
28  monetary value advertised in said one of said digital
29  advertisements and in order to initiate recordation of
30  said payment request and an authorization in a settlement
31  database;
32              at least one of said merchant computers being
33  programmed to receive said purchase message, and to cause
34  said product to be sent to said user conditioned on said
```

AMENDED SHEET (ARTICLE 19)

35   purchase transaction having been authorized in real time
36   by a financial authorization network external to said
37   network sales system, based on an external credit card
38   account or an external demand deposit account having
39   sufficient credit or funds of real monetary value
40   available to said principal making said payment, and
41   conditioned on at least one message transmitted over said
42   public packet switched communications network in
43   connection with purchase of said product not being a
44   replay of a message previously transmitted over said
45   public packet switched communications network.

1   2.   A network sales system in accordance with
2   claim 1, wherein said payment system is configured to
3   perform a replay check of said payment request to
4   determine whether an identical payment request was
5   previously transmitted to said payment system.

1   3.   A network sales system in accordance with
2   claim 1, wherein said payment system verifies an
3   authenticator in order to verify said identity of said
4   principal making payment.

1   4.   A network sales system in accordance with
2   claim 3, wherein said payment system, upon verification
3   of said authenticator, sends an authorization request to
4   said financial authorization network and receives
5   authorization from said financial authorization network.

1   5.   A network sales system in accordance with
2   claim 1, wherein at least one of said merchant computers
3   is programmed to communicate a missing payment
4   information request message to said buyer computer to
5   obtain missing payment information, said buyer computer
6   is programmed to query a user for said missing payment

AMENDED SHEET (ARTICLE 19)

7   information and to transmit said missing payment
8   information to at least one of said merchant computers.

1   6. A network sales system in accordance with
2   claim 1, wherein said payment request comprises a payment
3   order that describes the identity of a sender, a payment
4   amount, a beneficiary, and a nonce.

1   7. A network sales system in accordance with
2   claim 1, wherein said payment system is external to said
3   plurality of buyer computers and said plurality of
4   merchant computers.

1   8. A network sales system in accordance with
2   claim 1, wherein said demand deposit account comprises a
3   debit card account.

1   9. A network payment system for transferring
2   funds having real monetary value from a sender to a
3   beneficiary and providing for real-time authorization of
4   payment transactions by a financial authorization network
5   external to said network payment system, comprising:
6   a plurality of client computers; and
7   at least one payment computer;
8   said client computers and said payment computer
9   being interconnected by a public packet switched
10 communications network;
11   each one of said client computers being programmed
12 to construct a payment request specifying a payment
13 amount to be transferred from a sender to a beneficiary,
14 and to cause said payment request to be transmitted to
15 said payment computer;
16   said payment computer being programmed to cause a
17 message to be transmitted into said financial
18 authorization network external to said network payment

19 system in order to verify that said sender has adequate
20 funds or credit having real monetary value, to receive an
21 authorization from said financial authorization network
22 in response to said message, to transmit an authorization
23 message to said client computer, to cause said payment
24 request and authorization to be recorded in a settlement
25 database, and to cause funds having real monetary value
26 to be transferred from said sender to said beneficiary
27 conditioned on said payment request having been
28 authorized in real time by said financial authorization
29 network based on an external credit card account or an
30 external demand deposit account having sufficient credit
31 or funds of real monetary value available to said sender,
32 and conditioned on at least one message transmitted over
33 said public packet switched communications network in
34 connection with transfer of said funds not being a replay
35 of a message previously transmitted over said public
36 packet switched communications network.

1   10. A network payment system in accordance with
2 claim 9, wherein said payment computer is programmed to
3 perform a replay check of said payment request to
4 determine whether an identical payment request was
5 previously transmitted to said payment computer.

1   11. A network payment system in accordance with
2 claim 9, wherein said payment request comprises at least
3 a partial delivery address, and wherein said payment
4 computer is programmed to cause said delivery address to
5 be checked against a database of allowed delivery
6 addresses for said sender.

1   12. A network payment system in accordance with
2 claim 9, wherein said payment computer is programmed to
3 cause at least partial allowed delivery addresses for

AMENDED SHEET (ARTICLE 19)

4   said sender to be determined, and wherein said
5   authorization message comprises said at least partial
6   allowed delivery addresses.

1   13.   A network payment system in accordance with
2   claim 9, wherein said authorization message comprises an
3   authenticator.

1   14.   A network payment system in accordance with
2   claim 9, wherein said client computer is programmed to
3   cause an authenticator that verifies to said payment
4   computer the identity of said sender to be transmitted to
5   said payment computer, and wherein said payment computer
6   is programmed to examine said authenticator to verify
7   said identity of said sender.

1   15.   A network payment system in accordance with
2   claim 14, wherein said client computer is programmed to
3   generate a next expected transaction identifier for said
4   sender and to use it to create said authenticator, and
5   wherein said payment computer is programmed to generate
6   said next expected transaction identifier for said sender
7   and to verify that said authenticator was created using
8   said next expected transaction identifier.

1   16.   A network payment system in accordance with
2   claim 14, wherein said client computer is programmed to
3   generate said authenticator using an external device, and
4   wherein said payment computer is programmed to verify
5   that said authenticator was created using said external
6   device.

1   17.   A network payment system in accordance with
2   claim 14, wherein said payment request comprises a
3   network address of said client computer, and wherein said

AMENDED SHEET (ARTICLE 19)

4   payment computer is programmed to verify that said
5   payment request was constructed at said network address.

1   18.   A network payment system in accordance with
2   claim 13, wherein said payment request comprises a
3   network address of said client computer, and wherein said
4   payment computer is programmed to check said network
5   address against a database of allowed client addresses
6   for said sender.

1   19.   A network payment system in accordance with
2   claim 9, wherein said payment computer is programmed to
3   determine whether real-time authorization is necessary
4   and to cause said message to be transmitted into said
5   financial authorization network to verify that said
6   sender has adequate funds or credit only if said payment
7   computer has determined that real-time authorization is
8   necessary.

1   20.   A network payment system in accordance with
2   claim 9, wherein said demand deposit account comprises a
3   debit card account.

1   21.   A method of effecting sales over a network
2   sales system comprising a plurality of buyer computers
3   and a plurality of merchant computers interconnected by a
4   public packet switched communications network, said
5   method providing for real-time authorization of purchase
6   transactions and comprising the steps of:
7   storing digital advertisements in a database;
8   receiving a user inquiry at one of said buyer
9   computers and, in response to said user inquiry,
10 selecting one of said merchant computers, and
11 transmitting a network request from said one of said
12 buyer computers thereto;

AMENDED SHEET (ARTICLE 19)

13   communicating one of said digital advertisements
14   from one of said merchant computers to said one of said
15   buyer computers over said public packet switched
16   communications network in response to said network
17   request from said buyer computer;
18   displaying said one of said digital advertisements
19   at said one of said buyer computers, and, in response to
20   a user request, transmitting from said one of said buyer
21   computers to one of said merchant computers a purchase
22   message, and causing a payment request, comprising a
23   payment amount, to be transmitted into a payment system
24   in order to initiate authorization of purchase of a
25   product having real monetary value advertised in said one
26   of said digital advertisements and in order to initiate
27   recordation of said payment request and an authorization
28   in a settlement database; and
29   receiving said purchase message at one of said
30   merchant computers, and causing said product to be sent
31   to said user conditioned on said purchase transaction
32   having been authorized in real time by a financial
33   authorization network external to said network sales
34   system, based on an external credit card account or an
35   external demand deposit account having sufficient credit,
36   or funds of real monetary value available to said
37   principal making said payment, and conditioned on at
38   least one message transmitted over said public packet
39   switched communications network in connection with said
40   purchase transaction not being a replay of a message
41   previously transmitted over said public packet switched
42   communications network.

1   22. A method in accordance with claim 21, further
2   comprising the step of performing a replay check, at said
3   payment system, of said payment request to determine

4 whether an identical payment request was previously
5 transmitted to said payment system.

1   23. A method in accordance with claim 21, wherein
2 said method further comprises the steps of verifying, at
3 said payment computer, an authenticator in order to
4 verify said identity of said principal making payment.

1   24. A method in accordance with claim 23, further
2 comprising the steps of, upon verification of said
3 authenticator, sending an authorization request from said
4 payment computer to said financial authorization network,
5 and receiving at said payment computer authorization from
6 said financial authorization network.

1   25. A method in accordance with claim 21, further
2 comprising the steps of communicating a missing payment
3 information request message from one of said merchant
4 computers to said buyer computer to obtain missing
5 payment information, querying a user for said missing
6 payment information, and transmitting said missing
7 payment information from said buyer computer to one of
8 said merchant computers.

1   26. A method in accordance with claim 21, wherein
2 said payment request comprises a payment order that
3 describes the identity of a sender, a payment amount, a
4 beneficiary, and a nonce.

1   27. A method in accordance with claim 21, wherein
2 said payment system is external to said plurality of
3 buyer computers and said plurality of merchant computers.

1   28.   A method in accordance with claim 21, wherein
2   said demand deposit account comprises a debit card
3   account.

1   29.   A method of transferring funds having real
2   monetary value from a sender to a beneficiary using a
3   network payment system comprising a plurality of client
4   computers and at least one payment computer
5   interconnected by a public packet switched communications
6   network, said method providing for real-time
7   authorization of purchase transactions by a financial
8   authorization network external to said network payment
9   system and comprising the steps of:
10   constructing a payment request at one of said
11   client computers specifying a payment amount to be
12   transferred from a sender to a beneficiary, and causing
13   said payment request to be transmitted to said payment
14   computer; and
15   causing a message to be transmitted into said
16   financial authorization network external to said network
17   payment system in order to verify that said sender has
18   adequate funds or credit having real monetary value,
19   receiving, at said payment computer, an authorization
20   from said financial authorization system in response to
21   said message, transmitting an authorization message from
22   said payment computer to said client computer, causing
23   said payment request and authorization to be recorded in
24   a settlement database, and causing funds having real
25   monetary value to be transferred from said sender to said
26   beneficiary conditioned on said payment request having
27   been authorized in real time by said financial
28   authorization system based on an external credit card
29   account or an external demand deposit account having
30   sufficient credit or funds of real monetary value
31   available to said sender, and conditioned on at least one

AMENDED SHEET (ARTICLE 19)

32   message transmitted over said public packet switched
33   communications network in connection with transfer of
34   said funds not being a replay of a message previously
35   transmitted over said public packet switched
36   communications network.

1   30.   A method in accordance with claim 29, further
2   comprising the step of performing a replay check, at said
3   payment computer, of said payment request to determine
4   whether an identical payment request was previously
5   transmitted to said payment computer.

1   31.   A method in accordance with claim 29, wherein
2   said payment request comprises at least a partial
3   delivery address, and wherein said method further
4   comprises the step of checking said delivery address
5   against a database of allowed delivery addresses for said
6   sender.

1   32.   A method in accordance with claim 29, further
2   comprising the steps of determining at least partial
3   allowed delivery addresses for said sender, and wherein
4   said authorization message comprises said at least
5   partial allowed delivery addresses.

1   33.   A method in accordance with claim 29, wherein
2   said authorization message comprises an authenticator.

1   34.   A method in accordance with claim 29, wherein
2   further comprising the steps of causing an authenticator
3   that verifies to said payment computer the identity of
4   said sender to be transmitted to said payment computer,
5   and examining said authenticator at said payment computer
6   to verify said identity of said sender.

AMENDED SHEET (ARTICLE 19)

1   35. A method in accordance with claim 34, further
2   comprising the steps of generating, at said client
3   computer, a next expected transaction identifier for said
4   sender and using it to create said authenticator, and
5   generating, at said payment computer said next expected
6   transaction identifier for said sender, and verifying, at
7   said payment computer, that said authenticator was
8   created using said next expected transaction identifier.

1   36. A method in accordance with claim 34, further
2   comprising the steps of generating said authenticator at
3   said client computer using an external device, and
4   verifying, at said payment computer that said
5   authenticator was created using said external device.

1   37. A method in accordance with claim 34, wherein
2   said payment request comprises a network address of said
3   client computer, and wherein said method further
4   comprises verifying, at said payment computer, that said
5   payment request was constructed at said network address.

1   38. A method in accordance with claim 29, wherein
2   said payment request comprises a network address of said
3   client computer, and wherein said method further
4   comprises the step of checking, at said payment computer,
5   said network address against a database of allowed client
6   addresses for said sender.

1   39. A method in accordance with claim 29, further
2   comprising the steps of determining, at said payment
3   computer, whether real-time authorization is necessary,
4   and causing said message to be transmitted into said
5   financial authorization network to verify that said
6   sender has adequate funds or credit only if said payment

AMENDED SHEET (ARTICLE 19)

7   computer has determined that real-time authorization is
8   necessary.

1   40.   A method in accordance with claim 29, wherein
2   said demand deposit account comprises a debit card
3   account.

1   41.   A network sales system providing for real-
2   time authorization of purchase transactions, comprising:
3   a plurality of buyer computers; and
4   a plurality of merchant computers;
5   said plurality of buyer computers and said
6   plurality of merchant computers being interconnected by a
7   public packet switched communications network;
8   each of said buyer computers being programmed to
9   transmit to at least one of said merchant computers, in
10 response to a user request, a purchase message and to
11 cause a payment request, comprising a payment amount, to
12 be transmitted into a payment system in order to initiate
13 authorization of purchase of a product having real
14 monetary value and in order to initiate recordation of
15 said payment request and an authorization in a settlement
16 database;
17   at least one of said merchant computers being
18 programmed to receive said purchase message, and to cause
19 said product to be sent to said user conditioned on said
20 purchase transaction having been authorized in real time
21 by a financial authorization network external to said
22 network sales system, based on an external credit card
23 account or an external demand deposit account having
24 sufficient credit or funds of real monetary value
25 available to a principal making said payment, and
26 conditioned on at least one message transmitted over said
27 public packet switched communications network in
28 connection with purchase of said product not being a

AMENDED SHEET (ARTICLE 19)

29   replay of a message previously transmitted over said
30   public packet switched communications network.

1   42.   A method of effecting sales over a network
2   sales system comprising a plurality of buyer computers
3   and a plurality of merchant computers interconnected by a
4   public packet switched communications network, said
5   method providing for real-time authorization of purchase
6   transactions and comprising the steps of:
7   in response to a user request, transmitting from
8   one of said buyer computers to one of said merchant
9   computers a purchase message, and causing a payment
10   request, comprising a payment amount, to be transmitted
11   into a payment system in order to initiate authorization
12   of purchase of a product having real monetary value and
13   in order to initiate recordation of said payment request
14   and an authorization in a settlement database; and
15   receiving said purchase message at one of said
16   merchant computers, and causing said product to be sent
17   to said user conditioned on said purchase transaction
18   having been authorized in real time by a financial
19   authorization network external to said network sales
20   system, based on an external credit card account or an
21   external demand deposit account having sufficient credit
22   or funds of real monetary value available to a principal
23   making said payment, and conditioned on at least one
24   message transmitted over said public packet switched
25   communications network in connection with said purchase
26   transaction not being a replay of a message previously
27   transmitted over said public packet switched
28   communications network.

AMENDED SHEET (ARTICLE 19)

STATEMENT UNDER ARTICLE 19

In response to the search report the existing claims have been cancelled and new claims have been introduced. Replacement pages have been provided with this amendment. If there are any charges or credits not covered, please apply them to Deposit Account No. 06-1050. Any inquiry concerning this communication may be directed to the undersigned at the telephone number provided below.